ISO - International Organisation for Standardisation
IEC - International Electrotechnical Commission

JTC 1 - "Information Technology"
SC 27 - "Security Techniques"
WG 3 - "Security Evaluation Criteria"

TITLE: Liaison statement to the Common Criteria Interpretations Management Board

SOURCE: ISO/IEC JTC 1/SC 27/WG 3 Meeting, Madrid, April 1999

DATE: 1999-04-23

STATUS: For distribution to ISO/IEC JTC 1/SC 27

LIAISON STATEMENT

FROM: ISO/IEC JTC 1/SC 27/WG 3
TO: THE COMMON CRITERIA INTERPRETATIONS MANAGEMENT BOARD (CCIMB)

1. Expression of Thanks

ISO/IEC JTC 1/SC 27/WG 3 thanks the CCIMB Liaison Officer Ulrich van Essen for the report and presentation on the progress, status and plans for the CC project (WG 3 N470) and Lynne Ambuel for the comprehensive presentation on the Common Methodology for IT Security Evaluation (CEM).

2. Ballot on the Final Draft International Standard

The ballot on the Final Draft International Standard ISO/IEC 15408 has begun on April 1st, 1999 and will end on June 1st, 1999. Provided that sufficient support is received in this ballot, the document will be published as an International Standard.

3. Editorial Changes after the October 1998 meeting

The liaison statement sent to the CCIMB after the WG 3 meeting in October 1998 contained a list of editorial changes. These changes represent the difference between the CC version 2.0 published in May 1998 and the Final Draft International Standard that was sent to ISO in November 1998. Subsequently the ISO authority ITTF provided editorial comments (e.g. use of certain headlines and footers, replacing the word ”chapter” by ”clause” etc.). These were implemented in co-operation with the CCIMB and the revised draft was provided to ITTF in early January 1999 in both hardcopy and softcopy. The softcopy version was afterwards slightly changed by ITTF in an editorial manner.

WG 3 is interested in getting a complete overview of the changes that have been made since November 1998. In annex A there is a list of all the identified changes that have been made by ITTF after January 1999. WG 3 has already undertaken steps to obtain a softcopy of the version that is the basis for the final ballot with the intent to perform a file-compare with the version of the 15 November 1998 in order to get a complete overview of all changes made intermediately.

WG 3 suggests that this work be done in co-operation with the CCIMB in order to ensure that the shared responsibility, which is expressed in the legal notice in the Foreword of each part of ISO/IEC 15408, is guaranteed, and that all partners have a precise knowledge of its content.

4. Protection Profile Registration Authority

WG 3 is still in favour of a single international Registration Authority for the purpose of registering Protection Profiles. Meanwhile the French National Standardisation Body AFNOR has expressed its willingness to act as such an authority and the international industry standardisation organisation ECMA has expressed its interest to act as such an authority.

5. Criteria Maintenance

WG 3 encourages the CCIMB to use the information about the ISO maintenance rules with the intent to have as little divergence from those rules as possible. WG 3 requests that it be informed in due course about any relevant input the CCIMB could provide in this matter.

6. WG 3 Study Period on evaluation methodology

WG 3 received as valuable contribution from the CC project the Common Methodology for IT Security Evaluation (CEM) Part 2, version 0.6. WG 3 was informed about the current status of the CEM and subsequently discussed how to use this information for standardisation activities. WG 3 will continue the study period for an evaluation methodology to determine the standardisation work needed in this field.

WG 3 welcomes further contributions in this area provided by the CC project.

WG 3 has analysed annex C of the CEM in detail and offers comments, which are contained in annex B.

7. Availability of ISO/IEC 15408 on the Internet

Both JTC 1 and the ISO council endorsed the request of SC 27 last year to make ISO/IEC 15408 available on the Internet. The endorsement by the IEC has not yet been given, but IEC has been asked again by ISO recently to give an update in order to come to conclusion in this matter.

8. Guide on the production of PPs and STs

As a large number of National Body comments was received the document will undergo a major revision. The next draft of the Guide is due by July 1st, 1999.

Annex A, Overview over the editorial changes made by ITTF

(1) A sentence was added as a new second paragraph in the Foreword of each part

(2) In the Foreword the title of the document is cited in its exact form

(3) On page one, the headlines are presented in a different lay-out with four lines

(4) In the page number, the information about the total number of pages (”of nnn”) was deleted.

(5) French titles have been added to all three parts.

Annex B, Comments on the Common Methodology for IT Security Evaluation

The comments are ordered by issues as defined in annex C of the CEM Part 2, version 0.6.

Issue 1
The current structure of the CEM part 2 is focusing on the aspects on PP and ST evaluation as well as particular actions or considerations for each respective EAL. General issues are described in Annex B (Evaluation Techniques). WG 3 suggests that the document initially should describe basic evaluation principles (expanding the current text in Annex B). The parts of the text currently in the main body (PP, ST, EALs) should be placed in annexes.

Regarding potential future work of WG 3, the WG believes that there is a need for several documents rather than just the current one.

WG 3 believes that there is a clear need for a document dealing with Evaluation Methods, including a description of basic principles for evaluation work, general philosophy, methods for checking traceability and unambiguous language, supportive tools for code analysis, test coverage & tracing etc.

Issue 2

Use of FPT_SEP and FPT_RVM is related to the requirement to provide protection from interference for the TOE. Given that this is generally a requirement it is likely that these components will be called up for the majority of TOEs, implemented either within the TOE itself, or within the TOE's environment. Alternative approaches may utilise physical protection through use of FPT_PHP. Where the threat of interference to the security functions of the TOE is not cited within the PP/ST, then the evaluation should consider only the correct implementation of the security functions, and should not include determination of non-interference by other code, or bypass by an attacker. In other words, the threat statement should drive the evaluation effort. Preference is therefore given to the option described in C.3.2.3 of CEM 0.6.

Issues 4 and 8

Attack potential is directly related to threat and acceptable risk. The factors for determining the threat are many and complex and cannot be reduced to a mathematical algorithm. The CEM should adopt a threat model (as many are published and accepted as viable) and then relate that for determining attack potential and vulnerabilities. One area that should be expanded in the guidance in the CEM is that different factors have different weight for different types of evaluations. For instance, motivation is related to value of assets being protected. A system evaluation (within the end environment) will have more concrete knowledge of the asset value (or perception of the value) and motivation will play a large role in determining the threat to those assets.

Issue 5

In practice there may often be no direct correspondence between that which is evaluated and that which is delivered to the consumer. Products are often functionally rich, and vendors may choose to target evaluation on a subset of this functionality. It is therefore important to have a clear definition of TOE, as distinct from a delivered product. Preference is therefore given to the

alternative expressed in C.3.5.4 of CEM 0.6. A secondary issue was considered as to what action is required of an evaluator with respect to those parts of a product that are not within the scope of the TOE. It was determined that the evaluator should consider whether the limitation is valid, in terms of both the threats that the TOE is claimed to counter, and the CC functional dependencies that need to be met. In other words, the evaluator should determine that the evaluation results for the TOE are valid for the intended environment.

Issue 6

There is also a need for further guidance for evaluators on the application of CC part 3. Regarding issue 6 dealing with the structure of such guidance, WG 3 recognises the benefits of both approaches (EAL and class/family/component structure respectively). Even though specifically developed alternative Assurance Packages are not encouraged by the CC, this is still possible or in some contexts beneficial. WG 3 recommends that there should be a hypertext version of the text giving support to either way of use.

WG 3 also believes that more focus should be on the requirements on deliverables, and would like to see more worked examples in the documents annexes.

Issues 10 and 11

The ST bounds an evaluation and therefore the evaluator work. These bounds are often stated in the assumptions, especially as they relate to the environment. The evaluation need say nothing about any configurations or environments defined as being out of scope. Instead, the evaluation makes a statement as to whether the TOE meets the requirements stated in the ST, within the environment defined therein. This does not specifically mean that the TOE cannot be used in other environments, just that the user takes the risk of going beyond the constraints of the evaluation. The user purchases the TOE with the belief that the results hold if the assumptions hold true. Any change in the areas covered by the assumptions constitute additional risks. However, it must be very clear to the user what the evaluated configurations and environments for use are. The buyer can then make an informed decision whether they wish to take the risk of using the TOE outside the evaluated configuration.

The WG 3 experts agreed that it might be useful for the TOE purchaser to know of any known vulnerabilities discovered by the evaluator that would be exposed if the TOE is used differently than defined in the ST. However, this is beyond the scope of the evaluation. Requiring that the evaluator provides information on other environments would take the evaluation beyond the bounds defined. They agreed that the user guidance documents should only need to describe the evaluated configuration and cannot cover all possible configurations. The evaluators are required to report on vulnerabilities found, but only those bounded by the ST. What evaluators do with other vulnerabilities known (but beyond the scope of the evaluation) may be an issue for quality assurance within schemes and may be restricted by the contractual arrangements of the evaluation.

Issue 12

It is important that the consumer is able to gain benefit from the evaluation results, and is not misled with respect to operation of the TOE in a secure mode. Therefore it is considered essential that the consumer is provided with sufficient information to allow the TOE to be operated in a manner consistent with the evaluated configuration. This approach is consistent

with that taken under TPEP in the US. In the past European evaluations have relied upon consumers reading the ST or certification report. However, it is felt that the information should be made more readily available. Preference is therefore given to the alternative expressed in C.3.12.3 of CEM 0.6.

Issue 13
Many countries are considering to establish evaluation schemes. WG 3 recognises a need for a document describing minimum requirements on such schemes. The document may have a title like [Certification] Framework for Evaluation Schemes. The rationale for such a document should be to support mutual recognition on the administrative and procedural level. WG 3 would like to receive the views of the CC project on this issue.

General remarks
In summary, WG 3 believes that the current draft to some extent is dealing with issues which need to be covered in the area of CC Interpretations and/or CC Maintenance.

Guidance for evaluators is needed in the first hand from a purely technical viewpoint, enhancing quality and objectivity in the evaluation work. The fact that this is also important in the context of Mutual Recognition (MR) should not be a primary concern when defining supportive document(s) for evaluation work. It is expected that a sound technical basis for evaluation work will be helpful in a MR context (but there is no relation in the other direction).

WG 3 suggest using CC terminology whenever possible, and notes that, for example, the definition of ”Scheme” in CEM v 0.6 is different from CC definition of ”Evaluation Scheme”.